Assignment for Week 2: Amazon EC2 instance creation

Description

In this assignment your team will create a few Amazon EC2 virtual machine instances you'll be using for the rest of the course. You'll also explore some of the basic properties of an instance.

What you need to do

1. Create a key pair for yourself in the EC2 console under "Key Pairs". Click the "Create Key Pair" button and save the resulting key pair. *Be careful with this file!* Do not place it anywhere where other people can access it. For added protection, encrypt the private key with a password using "ssh-keygen -p" or the equivalent. See [Amazon EC2 Key Pairs](#) for more details on how to create and manage a personal key pair.
2. Launch three EC2 instances. Each team member needs to launch at least one instance. Use these properties for your instances:
   - Choose AMI: Use one of the "free tier" Linux machine images. One of the Ubuntu types is recommended but Red Hat and SUSE Linux are also available.
   - Choose Instance Type: t2.micro
   - Configure Instance Details:
     - Network: lab-cloud
     - Subnet: choose your team's subnet
   - Configure Security Group: Select an existing security group, then select "default (default VPC security group)"
   - Once you have selected all of these, you can finally launch the instance. Make sure to choose your own key pair for access and not somebody else's.
3. Obtain your own public key by logging in to your instance and getting the contents of the file .ssh/authorized_keys. Add access for your other team members by adding lines to .ssh/authorized_keys containing their public keys. You should be careful with this since you could lock yourself out of your instance if you damage that file. A recommended process:
   1. Log in to the session and back up the authorized_keys file: `cp .ssh/authorized_keys authorized_keys_backup`
   2. Edit the .ssh/authorized keys file to add a public key line from another team member. Make sure your editor doesn't wrap words or lines.
   3. You and your team member should try to initiate separate logins to the instance to be sure you can both get in.
   4. If you're not able to get in, use your existing login session to restore your backup: `cp authorized_keys_backup .ssh/authorized_keys`.

What to turn in

Create a subdirectory in your team git repository with the name "week2" and create files containing your handin materials under that.

1. List the EC2 instance IDs and private IP addresses of all the instances you created.
2. Describe how you find the public IP address of a given instance using the EC2 console. (The public IP address may change whenever an instance is stopped and restarted.)
3. Provide the output of a command showing how much disk space one of your instances has.
4. Provide the output of a command showing how much memory one of your instances has.
5. Provide a listing showing all the processes running in one of your instances.
6. Provide the output of a command showing the network interface configuration of your instance (this should show its private IP address).
7. Provide the output of a command showing the routing table of your instance.
8. Provide the outout of a command showing all of the open network connections and ports on one of your instances.
9. Provide a listing of all of the software packages installed on one your instances.
10. Provide transcripts showing the output of the commands you use to update your package database and upgrade packages on each of your instances.

Material for all of the above should be checked into your team git repository by class time on Monday, July 6.

Class presentation/discussion

On Monday, July 6 we will take some time in class to have everyone speak briefly about their experience with this assignment.

Evaluation

Each item under "What to turn in" is worth one point.

Steve VanDevender